REMARKS/ARGUMENTS

These remarks are made in response to the Office Action of April 15, 2009 (Office Action). As this response is timely filed within the 3-month shortened statutory period, no fee is believed due. However, the Examiner is expressly authorized to charge any deficiencies to Deposit Account No. 14-1437.

Claims Rejections – 35 USC § 101

Claims 1-4, 16-18, and 24-27 were rejected under 35 U.S.C. § 101 because it was asserted that the claimed invention is directed to non-statutory subject matter. Specifically, it was asserted that the claims recite an abstract idea only and the method steps can be performed in the mind of the user or by use of a pencil and paper.

Applicants respectfully disagree. The claims clearly recite a method and system that are tied to particular devices such as a central repository and an access device. The method cannot be performed in a user's mind or by use of a pencil and paper without the help of the particular devices.

In addition, Applicants submit that a person of ordinary skill in the art would readily appreciate that practicable embodiments of the claimed invention would be conducted with the aid of a computing machine, such as a server. Such computing machines are commonly understood to have memory. Further, the operations recited in the claims clearly change the state of the underlying data since the cache, register, or other memory on which the data is stored must be transformed to have a different magnetic polarity, electrical charge, or the like depending on the technology that is used. These are real physical changes. Further, memory is a real physical article. As such, Applicants submit that the method claims perform a transformation under the "machine or transformation" test and thus qualify as patent-eligible subject matter.

Claims 1 and 24 have been amended to recite a computer-implemented method and a computer-implemented system respectively in order to facilitate prosecution of the instant application.

Claims Rejections – 35 USC § 112

Claims 1-4, 16-18, and 20-27 were rejected under 35 U.S.C. § 112, second paragraph as being indefinite. Specifically, it was asserted that the "means plus function" language recited in the claims lacks sufficiently disclosed structure under 112, sixth paragraph.

Although Applicants disagree, Applicants have amended the claims to avoid using the "means plus function" language.

Claims Rejections – 35 USC § 103

Claims 1-4 and 20-27 were rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent 6,988,075 to Hacker, *et al.* (hereinafter Hacker) in view of non-patent literature, "Public Standards and Patients' Control: How to Keep Electronic Medical Records Accessible but Private," BMJ, Feb. 2001; 322, pages 283-287 to Mandl, *et al.* (hereinafter Mandl). Claims 16-18 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Hacker in view of Mandl, and further in view of U.S. Published Patent Application 2002/0010679 to Felsher (hereinafter Felsher).

Although Applicants respectfully disagree with the rejections, Applicants have amended the claims in an effort to even more clearly define the present invention and to facilitate prosecution of the instant application. The claim amendments are fully supported by the original disclosure and no new matter has been introduced.

Aspects of Applicants' Invention

It may be helpful to reiterate certain aspects recited in the claims prior to addressing the cited references. One aspect of the invention, as typified by Claim 1, is a

computer-implemented method of permitting controlled access to medical information of a patient.

The method can include supplying medical information of the patient to a central repository by the patient and any medical providers who have treated the patient; and storing and maintaining the medical information of the patient in the central repository.

The method also can include accessing the medical information by the patient from an access device using a unique patient identifier and a patient PIN; and controlling by the patient an authorization and a scope of access to the medical information by modifying an access control list within the patient's profile when the patient is connected to the central repository. The access control list lists each authorized user and the assigned role of each authorized user. The scope of access includes which items of medical information are available to an assigned role and how that information will be viewed.

The method further can include assigning each authorized user with a unique authorized user ID and an authorized user PIN; and tracking and notifying the patient of an identity of a user that accessed the medical information, information that was accessed by the user, and when the user accessed the information.

See, e.g., Specification, paragraphs [0008], [0023], and [0035].

The Claims Define Over The Prior Art

It was asserted in paragraph 25 on page 10 of the Office Action that Hacker discloses a system having a unique access identification means (i.e. unique ID) and also giving a pass phrase to access the system (i.e. pin). Hacker teaches providing the provider with appropriate means for input of the unique access identification for patient identification and access along with unique passphrases (i.e. pin) to access the patient information (Hacker: col. 7, 60-66).

Col. 7, lines 60-66 of Hacker reads:

> *Appropriate means for input of the unique access identification means, such as bar code readers (BCRs) 160 for bar coded cards and bracelets, can be used for patient identification and access. Particularly sensitive patient information can be passphrase protected so that the medical provider must get permission from the patient to gain access to it.*

As already discussed in the previous response, in Hacker the unique access identification means is used for patient identification and is thus unique to the patient. The passphrase is used to get permission from the patient to gain access to sensitive patient information. Therefore, in Hacker both the access identification means and the passphrase are unique to the patient whose information is being accessed. In contrast, in the present invention, aside from the unique patient identifier and the patient PIN provided to the patient, an authorized user, such as a medical provider, is provided with a unique authorized user ID and an authorized user PIN to access the patient information when the patient is not around (see, e.g., paragraph [0024] of the specification of the instant application).

It was asserted in paragraph 26 on pages 10-11 of the Office Action that Mandl discloses the patient having preferences about different parts of his/her medical history by providing authorization independently; furthermore teachings that patients grant different access rights to different providers based on their role and on the particular individual (Mandl: p. 284; section Confidentiality).

However, as already discussed in the previous responsess, although Mandl mentions that the patient can limit the information to specific providers and provides an override mechanism that is controlled by the patient, Mandl does not suggest using an access control list as the mechanism for controlling access. It is noted that granting different access rights to different providers based on their role is not the same as using an access control list as the mechanism for controlling access. The former is the result and the latter is the tool to achieve the result. More specifically, Mandl does not disclose

controlling by the patient an authorization and a scope of access to the medical information by modifying an access control list within the patient's profile when the patient is connected to the central repository, wherein the access control list lists each authorized user and the assigned role of each authorized user, and wherein the scope of access includes which items of medical information are available to an assigned role and how that information will be viewed, as recited in Claims 1, 20, and 24 of the instant application.

In addition, since Hacker does not provide an authorized user, such as a medical provider, with a unique authorized user ID and an authorized user PIN to access the patient information when the patient is not around, Hacker cannot track and notify the patient of an identity of a user who accessed the medical information, information that was accessed by the user, and when the user accessed the information. It is described in col. 7, line 66 to col. 8, line 3 of Hacker that the patient can also specify an emergency override of passphrase protection, and notification to the patient can be provided as to what information was released to emergency medical personnel, including time, location, pages accessed, etc. However, it is noted that the system of Hacker cannot track the identity of the user who accessed the medical information because the emergency medical personnel does not have an authorized user ID.

Accordingly, the cited references, alone or in combination, fail to disclose or suggest each and every element of Claims 1, 20, and 24. Applicants therefore respectfully submit that Claims 1, 20, and 24 define over the prior art. Furthermore, as each of the remaining claims depends from Claims 1, 20, or 24 while reciting additional features, Applicants further respectfully submit that the remaining claims likewise define over the prior art.

Applicants thus respectfully request that the claim rejections under 35 U.S.C. § 103 be withdrawn.

CONCLUSION

Applicants believe that this application is now in full condition for allowance, which action is respectfully requested. Applicants request that the Examiner call the undersigned if clarification is needed on any matter within this Amendment, or if the Examiner believes a telephone interview would expedite the prosecution of the subject application to completion.

Respectfully submitted,

NOVAK DRUCE + QUIGG LLP

Date: July 15, 2009

/Gregory A. Nelson/
Gregory A. Nelson, Registration No. 30,577
Yonghong Chen, Registration No. 56,150
Customer No. 40987
CityPlace Tower
525 Okeechobee Blvd., Fifteenth Floor
West Palm Beach, FL 33401
Telephone: 561.838.5229